Palo Alto Networks ML-Powered Next-Generation Firewall Specifications and Features Summary

Table 1: Firewall Performance and Capacities

Performance and Capacities	PA-7080[A]	PA-7050[A]	PA-5450[B]	PA-5430	PA-5420	PA-5410	PA-5280	PA-5260	PA-5250	PA-5220
Firewall throughput (App-ID, appmix)	635 Gbps	384.8 Gbps	200 Gbps	60.5 Gbps	51.1 Gbps	39 Gbps	55.2 Gbps	55.2 Gbps	36.7 Gbps	15.6 Gbps
Threat Prevention throughput (appmix)	387.6 Gbps	226.2 Gbps	152 Gbps	44.5 Gbps	32 Gbps	24.8 Gbps	31.4 Gbps	31.4 Gbps	21.4 Gbps	8.8 Gbps
IPsec VPN throughput	314.6 Gbps	192.2 Gbps	87 Gbps[C]	42 Gbps	28.7 Gbps	21 Gbps	26.3 Gbps	26.3 Gbps	18.4 Gbps	9.5 Gbps
New sessions per second	6,000,000	4,000,000	3,600,000[C]	370,000	370,000	295,000	505,000	505,000	368,000	155,000
Maximum sessions	416,000,000	245,000,000	100,000,000[C]	7,200,000	5,000,000	3,600,000	64,000,000	32,000,000	8,000,000	4,000,000
Virtual systems (base/max[D])	25/225		25/225	25/125	15/65	10/20	25/225	25/225	25/125	10/20
Hardware Specifications	**PA-7080**	**PA-7050**	**PA-5450**	**PA-5430**	**PA-5420**	**PA-5410**	**PA-5280**	**PA-5260**	**PA-5250**	**PA-5220**
Interfaces supported[E]	10/100/1000 (up to 120), SFP/ SFP+ (up to 80), QSFP+/ QSFP28 (up to 40)	10/100/1000 (up to 72), SFP/ SFP+ (up to 48), QSFP+/ QSFP28 (up to 24)	100/1000/10G Cu (up to 8), 1G/10G SFP/ SFP+ (up to 24), 40G/100G QSFP28 (up to 4)	1G/2.5G/5G/10G (8), 1G/10G SFP/SFP+ (12), 25G SFP28 (4), 40G/100G QSFP+/QSFP28 (4)			100/1000/10G Cu (4), 1G/10G SFP/SFP+ (16), 40G/100G QSFP28 (4)			100/1000/10G Cu (4), 1G/10G SFP/ SFP+ (16), 40G QSFP+ (4)
Management I/O	SFP/SFP+ MGT (2), SFP/SFP+ HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), RJ-45 serial console (1), Micro USB serial console (1)		SFP/SFP+ MGT (2), SFP/SFP+ HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), RJ-45 serial console (1), Micro USB serial console (1)	1G SFP out-of-band management (1), 1G SFP HA (2) 40G QSFP+ HA (1), RJ-45 serial console (1), Micro USB serial console (1)			10/100/1000 Cu (2), 10/100/1000 out-of-band management (1), RJ-45 console (1)			
							40G/100G QSFP28 HA (1)			(1) 40G QSFP+ HA
Size	19U, 19" standard rack (33.22" H x 24.66" D x 17.5" W)	9U, 19" standard rack (15.75" H x 23.75" D x 17.5" W) or 14U, 19" standard rack with optional PAN-AIRDUCT kit (24.5" H x 23.75" D x 17.5" W)	5U, 19" standard rack (8.75" H x 30.25" D x 17.38" W)	2U, 19" standard rack (3.45" H x 22.5" D x 17.34" W)			3U, 19" standard rack (5.25" H x 20.5" D x 17.25" W)			
Power supply	2500 W AC (2400 W/2700 W) (4 expandable to 8)	2500 W AC (2400 W/2700 W) (4)	2200 W AC or DC (2 expandable to 4)	1200 W AC or DC (1:1 fully redundant) (2)			1200 W AC or DC (1:1 fully redundant) (2)			
Redundant power supply	Yes		Yes							
Disk drives	240 GB SSD system drive, RAID1 (2)		System: 480 GB SSD, RAID1 | Log: 4 TB SSD (optional)	480 GB SSD pair, system storage			System: 240 GB SSD, RAID1 | Log: 2 TB HDD, RAID1			
Hot-swappable fans	Yes		Yes							

Table 1: Firewall Performance and Capacities (continued)

Performance and Capacities	PA-3440	PA-3430	PA-3420	PA-3410	PA-3260	PA-3250	PA-3220
Firewall throughput (App-ID, appmix)	24 Gbps	20.5 Gbps	16.9 Gbps	11.6 Gbps	7.8 Gbps	5.2 Gbps	4.4 Gbps
Threat Prevention throughput (appmix)	12.8 Gbps	10.5 Gbps	8.7 Gbps	5.9 Gbps	4.3 Gbps	2.7 Gbps	2.3 Gbps
IPsec VPN throughput	14.5 Gbps	12.2 Gbps	9.9 Gbps	6.8 Gbps	4.4 Gbps	2.7 Gbps	2.5 Gbps
New sessions per second	268,000	240,000	205,000	145,000	88,000	58,000	48,000
Maximum sessions	3,000,000	2,500,000	2,000,000	1,400,000	2,200,000	2,000,000	1,000,000
Virtual systems (base/max[D])	1/11	1/11	1/11	1/11	1/6		
Hardware Specifications	**PA-3440**	**PA-3430**	**PA-3420**	**PA-3410**	**PA-3260**	**PA-3250**	**PA-3220**
Interfaces supported[E]	1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)		1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)		10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)	10/100/1000 (12), 1G/10G SFP/SFP+ (8)	10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)
Management I/O	100/1000 out-of-band management port (1), 100/1000 high availability (2), 10G SFP+ high availability (1), RJ-45 console port (1), Micro USB (1)				10/100/1000 out-of-band management port (1), 10/100/1000 high availability (2), 10G SFP+ high availability (1), RJ-45 console port (1), Micro USB (1)		
Size	1U, 19" standard rack 14.15" x 17.15" x 1.70"				2U, 19" standard rack (3.5" H x 20.53" D x 17.34" W)		
Power supply	450W AC				650 W AC or DC (180/240)		
Redundant power supply	Yes				Yes		
Disk drives	480 GB SSD				240 GB SSD		
Hot-swappable fans	Yes				Yes		

Performance and Capacities	PA-850	PA-820	PA-460	PA-450	PA-440	PA-410	PA-220	PA-220R
Firewall throughput (App-ID, appmix)	2.0 Gbps	1.5 Gbps	4.4 Gbps	3.0 Gbps	2.2 Gbps	1.2 Gbps	535 Mbps	535 Mbps
Threat Prevention throughput (appmix)	1.0 Gbps	840 Mbps	2.4 Gbps	1.6 Gbps	1.0 Gbps	685 Mbps	320 Mbps	320 Mbps
IPsec VPN throughput	1.8 Gbps	1.4 Gbps	3.0 Gbps	2.2 Gbps	1.7 Gbps	930 Mbps	550 Mbps	550 Mbps
New sessions per second	13,100	8,100	73,000	51,000	37,000	12,000	4,200	4,200
Maximum sessions	192,000	128,000	400,000	300,000	200,000	64,000	64,000	64,000
Virtual systems (base)	1	1	1	1	1	1	1	1
Hardware Specifications	**PA-850**	**PA-820**	**PA-460**	**PA-450**	**PA-440**	**PA-410**	**PA-220**	**PA-220R**
Interfaces supported[E]	10/100/1000 (4), 1G SFP (4), 1G/10G SFP/SFP+ (4)	10/100/1000 (4), SFP (8)	10/100/1000 (8)			10/100/1000 (7)	10/100/1000 (8)	10/100/1000 (6), SFP (2)
Management I/O	10/100/1000 out-of-band management (1), 10/100/1000 high availability (2), RJ-45 console (1), USB (1), Micro USB console (1)		10/100/1000 out-of-band management (1), RJ-45 console (1), USB (2), Micro USB console (1)			10/100/1000 out-of-band management (1), RJ-45 console (1), USB (2)	10/100/1000 out-of-band management (1), RJ-45 console (1), USB (1), Micro USB console (1)	
Size	1U, 19" standard rack (1.75" H x 14.5" D x 17.125" W)	1U, 19" standard rack (1.75" H x 14" D x 17.125" W)	1.74" H x 8.83" D x 8.07" W			1.63" H x 6.42" D x 9.53" W	1.62" H x 6.29" D x 8.07" W	2.0" H x 8.66" D x 9.25" W
Power supply	450 W AC (2; one is redundant)	200 W	Dual redundant 50 W			25 W	Dual redundant 40 W	No ne
Redundant power supply	Yes	No	Yes (optional)			No	Yes (optional)	None
Disk drives	240 GB SSD		128 GB eMMC			64 GB eMMC	32 GB eMMC	32 GB eMMC
Hot-swappable fans	No		Fanless				Fanless	

(A) Each result in this column is for an optimum combination of PA-7000-DPC-A and PA-7000-100G-NPC-A cards populated in all available slots. (B) All tests performed with 2 Networking Cards + 4 Data Processing Cards populated, unless otherwise noted. (C) This test performed with 1 Networking Card + 5 Data Processing Cards populated. (D) Adding virtual systems to the base quantity requires a separately purchased license. (E) Optical/Copper transceivers are sold separately.

Table 2: Key Features	
Next-Generation Firewall	**Supported Across All Models**
Deep visibility and granular control for thousands of applications; ability to create custom applications; ability to manage unknown traffic based on policy	✓
User identification and control: VPNs, WLAN controllers, captive portal, proxies, Active Directory, eDirectory, Exchange, Terminal Services, syslog parsing, XML API	✓
Granular TLS/SSL decryption and inspection (inbound and outbound); includes support for TLS 1.3 and HTTP/2 protocols	✓
Networking: dynamic routing (RIP, OSPF, BGP, multiprotocol BGP), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, tunnel content inspection	✓
QoS: policy-based traffic shaping (priority, guaranteed, maximum) per application, per user, per tunnel, based on DSCP classification	✓
Virtual systems: logical, separately managed firewall instances within a single physical firewall, with each virtual system's traffic kept separate	✓
Zone-based network segmentation and zone protection; DoS protection against flooding of new sessions	✓
Threat Prevention (subscription required)	
Inline malware prevention automatically enforced through payload-based signatures, updated daily	✓
Vulnerability-based protections against exploits and evasive techniques on network and application layers, including port scans, buffer overflows, packet fragmentation, and obfuscation	✓
Command-and-control (C2) activity stopped from exfiltrating data or delivering secondary malware payloads; infected hosts identified through DNS sinkholing	✓
URL Filtering (subscription required)	
Automatic prevention of web-based attacks, including phishing links in emails, phishing sites, HTTP-based C2, and pages that carry exploit kits	✓
Ability to stop in-process credential phishing	✓
Custom URL categories, alerts, and notification pages	✓
IoT Security (subscription required)	
Accurate identification and classification of all devices on a network, including never-before-seen devices	✓
Device security via ML-based anomaly detection, vulnerability assessment, risk-based policy recommendations, and enforcement with the Device-ID policy construct (Device-based policy enforcement not available on the VM-50, VM-50 Lite, or CN-Series)	✓
No additional infrastructure required to enable on Next-Generation Firewalls	✓
WildFire malware prevention (subscription required)	
Detection of zero-day malware and exploits with layered, complementary analysis techniques	✓
Automated prevention in seconds for most threats across networks, endpoints, and clouds	✓
Community-based data for protection, including more than 30,000 subscribers	✓
AutoFocus threat intelligence (subscription required)	
Contextualization and classification of attacks, including malware family, adversary, and campaign, to speed triage and response efforts	✓
Rich, globally correlated threat analysis sourced from WildFire	✓
Third-party threat intelligence for automated prevention	✓
DNS Security (subscription required)	
Automatic prevention of tens of millions of malicious domains identified with real-time analysis and continuously growing global threat intelligence	✓
Quick detection of C2 or data theft employing DNS tunneling with machine learning-powered analysis	✓
Automated dynamic response to find infected machines and quickly respond in policy	✓
File and data filtering	
Bidirectional control over the unauthorized transfer of file types and Social Security numbers, credit card numbers, and custom data patterns	✓
GlobalProtect network security for endpoints (subscription required)	
Remote access VPN (SSL, IPsec, clientless); mobile threat prevention and policy enforcement based on apps, users, content, device, and device state	✓
BYOD: app-level VPN for user privacy	✓
Panorama network security management (subscription required for managing multiple firewalls)	
Intuitive policy control with applications, users, threats, advanced malware prevention, URLs, file types, and data patterns all in the same policy	✓
Actionable insight into traffic and threats with Application Command Center (ACC); fully customizable reporting	✓
Aggregated logging and event correlation	✓
Consistent scalable management of up to 30,000 hardware and all VM-Series Firewalls; role-based access control; logical and hierarchical device groups; and templates	✓
GUI, CLI, XML-based REST API	✓